ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits d'Adobe
Numéro de Référence	36821506/22
Date de Publication	15 Juin 2022
Risque	Important
Impact	Critiques

Systèmes affectés

- Adobe Bridge 12.0.1 et versions antérieures sur Windows et macOS
- Illustrator 2021 version 25.4.5 et versions antérieures
- Illustrator 2022 version 26.0.2 et versions antérieures
- Adobe InDesign 17.2.1 et versions antérieures
- Adobe InDesign 16.4.1 et versions antérieures
- Adobe RoboHelp Server RHS 11 Update 3et versions antérieures sur Windows
- Adobe InCopy 17.2 et versions antérieures
- Adobe InCopy 16.4.1 et versions antérieures

Identificateurs externes

CVE-2022-28839	CVE-2022-28840	CVE-2022-28841	CVE-2022-28842
CVE-2022-28843	CVE-2022-28844	CVE-2022-28845	CVE-2022-28846
CVE-2022-28847	CVE-2022-28848	CVE-2022-28849	CVE-2022-28850
CVE-2022-30664	CVE-2022-28837	CVE-2022-28838	CVE-2022-30666
CVE-2022-30667	CVE-2022-30667	CVE-2022-30668	CVE-2022-30669
CVE-2022-30651	CVE-2022-30652	CVE-2022-30653	CVE-2022-30654
CVE-2022-30655	CVE-2022-30656	CVE-2022-30657	CVE-2022-30658
CVE-2022-30659	CVE-2022-30660	CVE-2022-30661	CVE-2022-30662
CVE-2022-30663	CVE-2022-30665	CVE-2022-30670	

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Bilan de la vulnérabilité

Adobe a publié des mises à jour de sécurité qui permettent de corriger plusieurs vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire, l'accès à des données confidentielles ou l'élévation de privilèges.

Solution

Veuillez se référer aux bulletins de sécurité d'Adobe pour l'obtention des correctifs.

Risque

- Exécution de code arbitraire
- Accès à des données confidentielles
- Elévation de privilèges

Référence

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/animate/apsb22-24.html
- https://helpx.adobe.com/security/products/bridge/apsb22-25.html
- https://helpx.adobe.com/security/products/illustrator/apsb22-26.html
- https://helpx.adobe.com/security/products/incopy/apsb22-29.html
- https://helpx.adobe.com/security/products/indesign/apsb22-30.html
- https://helpx.adobe.com/security/products/robohelp-server/apsb22-31.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma